American Journal of Mobile Systems, Applications and Services
Vol. 2, No. 1, 2016, pp. 1-12
http://www.aiscience.org/journal/ajmsas

Bandwidth Management and Loop Prevention in Redundant Networks

Isiaka A. Alimi*

Department of Electrical and Electronics Engineering, School of Engineering and Engineering Technology, Federal University of Technology, Akure, Nigeria

Abstract

The current multimedia applications and services effective functionalities require reliable network connectivity that can be achieved with the implementation of network redundancy. However, the redundancy may cause broadcast storm which results in an unstable and congested network because of the network loop. Spanning-Tree Protocol (STP) is a feasible technology for loop prevention in switched networks. It employs the IEEE 802.1D algorithm to exchange the bridge protocol data unit (BPDU) messages to detect and prevent the loops by blocking certain redundant interfaces. However, the associated bandwidths of the blocked interfaces are not being utilized in the network. Therefore, to enhance system performance, physical redundant links can be logically grouped into one in order to exploit the available bandwidth with the aid of EtherChannel. This paper presents STP concepts and its implementations in switched networks. Furthermore, how the root bridge election process can be managed in a network is demonstrated and finally, practical application of an EtherChannel for bandwidth aggregation is presented.

Keywords

STP, BPDU, Protocol, EtherChannel, Bridge ID, Root Bridge

Received: September 10, 2015 / Accepted: October 18, 2015 / Published online: January 11, 2016

1. Introduction

Computer network is an integral part of communication system development and also enables timely access to various information. Similarly, the significant transformations in multimedia applications and services such as e-commerce, e-government, e-banking, e-business, e-learning, real-time images or video and telemedicine have made the internet, which is a massive network of networks the most prominent tool for information dissemination worldwide [1]. To harness the advantages of these applications and services, there is need for high availability and reliable network connectivity [2]. To achieve the required availability, appropriate level of redundancy is essential for near immediate data-flow recovery by quickly swapping the network operations onto redundant infrastructure in case of any network component or link failure [1].

It has been observed in [1] that, high availability is the principal service requirement in designing an enterprise network. Also, system availability can be considerably enhanced in hierarchical networks by the implementation of redundancy. Network redundancy is a fault-tolerant approach in which additional network components and links are employed in a network to improve system reliability [3]. This approach ensures network availability in case of network components and links failure and also protects the network against a single point of failure (SPOF) which may render the entire system unavailable or unreliable. The internet, as the network of networks is made up of redundant resources such as standby routers, switches and additional links, which can be used to improve network robustness and protect the network against SPOF. Therefore, when the primary network component or link is inaccessible, then, the standby or alternate one can be employed instead to ensure minimal

* Corresponding author
E-mail address: compeasywalus2@yahoo.com

downtime and continuity in the network services [4].

The continuity of network services in switched networks can be achieved by having redundant links between switches. However, the redundancy may result in layer 2 technical issues such as mislearning MAC addresses, multiple frame copies, and broadcast storm which is a condition in which the broadcasts continuously circling the network [5]. This results in network loop in which network frame cycles around the network infinitely causing a huge volume of traffic from the broadcast frame and consumes almost all of the possible network bandwidth. This situation is due to the fact that there is more than one active path between two network devices and occurrence of multiple active paths results in an unstable and congested network. The loop can be prevented in a switched network with the aid of Spanning-Tree Protocol (STP). The STP is a layer 2 link management protocol that helps in maintaining network efficiency and preventing network loops occurrence when infrastructure devices such as switches and bridges are interconnected via multiple paths [6], [7]. The loop avoidance is realized by employing the IEEE 802.1D algorithm to exchange the bridge protocol data unit (BPDU) messages between adjacent switches at regular intervals to detect loops in the network and removes the loop by blocking the selected interfaces [6], [8]. However, the algorithm permits redundant paths to be automatically activated when the primary path goes down or becomes congested to ensure system availability [9].

This paper investigates loop prevention algorithms and bandwidth management in redundant networks by the implementation of spanning tree and EtherChannel. The STP concepts for switched networks and the standard variants are discussed in the subsequent Section. Moreover, root bridge election process as well as port roles and states are presented in Section 3. Section 4 focusses on the EtherChannels and the associated aggregation protocols. In Section 5, implementation of STP and a practical means of managing the root bridge election process are presented. Furthermore, it demonstrates the application of EtherChannels for bandwidth aggregation. Some concluding remarks are given in Section 6.

2. Spanning Tree Protocol

One of the major challenges of a switched network is the way by which the network loop can be prevented. The loop avoidance approach is a means of preventing the network frame from cycling around the network as well as optimizing the network bandwidth. The fundamental approach to prevent loops is to have a single path between switches in the entire network. Conversely, this approach prevents network scalability. Therefore, deployment of redundant paths is required in a large switched networks. In this type of network, the main challenge is controlling the potential loops that could be caused by the redundant paths. The Spanning Tree Protocol (STP) addresses the issue of potential loops in the entire switched network. To achieve this, redundant paths between switches are temporarily blocked in a normal operation. However, the redundant paths are automatically activated when the primary path goes down [9], [10]. Therefore, the STP helps in creating fault-tolerant and high availability internetworks which are the principal service requirement in designing an enterprise network. The plug-and-play property as well as ease of configuration of STP have been part of the fundamental success of the Ethernet [11], [12]. Nonetheless, the timer based property of STP results in low convergence time and consequently affects network performance. To achieve faster convergence, there have been several revisions to the original STP such as, the Rapid Spanning Tree protocol (RSTP) and the Multiple Spanning Tree Protocol (MSTP) [7], [12], [13], [14], [15]. Table 1 presents different STP standards and protocols.

Table 1. STP Standard Variants (Adapted from [16]).

	Protocol	Standard	Description	Calculation
IEEE Standard	STP	802.1D	Spanning Tree Protocol. Provides a loop-free topology.	All VLANs
	RSTP	802.1w	Rapid Spanning Tree Protocol. Provides faster convergence than STP.	All VLANs
	CST	802.1Q	Common Spanning Tree. One spanning-tree instance for the entire network.	All VLANs
	MSTP or MISTP	802.1s	Multiple (Instance) Spanning Tree Protocol. Inspired by the earlier Cisco proprietary MISTP. Maps multiple VLANs to a reduced number of instances.	Per instance
Cisco Proprietary	PVST PVST+	Cisco	Per-VLAN Spanning Tree Plus. Provides a separate STP instance for each VLAN. It has the ability to load balance traffic at layer-2.	Per VLAN
	PVRST+ RPVST+	Cisco	Rapid Per-VLAN Spanning Tree Plus. Cisco enhancement of RSTP that uses PVST+.	Per VLAN

2.1. STP Concepts

The fundamental purpose of implementing the STP is to offer a loop-free switched network. To achieve this objective, the topology information of all participating STP switches is first created and the acquired information is then employed to determine the best loop-free path through the switched network. Through the information, the root bridge election can be accomplished. The election process is determined by the bridge priority and the root bridge is the central point in a switched network to determine the best route through the network [10]. By this means, the STP defines a specific tree

with a root bridge and also offers a loop-free path from the root to all infrastructure devices in the network [6].

Furthermore, to determine which port will be in forwarding state or in the blocking state in a situation where there are two interfaces on a bridge that are part of a loop, the spanning-tree port priority and path cost settings are employed [8]. The port priority value signifies the location of an interface in the network topology while the path cost value represents the media speed. The redundant data paths in the network are forced into a standby (blocked) state by the STP. However, when a network segment in the spanning tree fails, the algorithm determines the spanning-tree topology again and activates the standby path in the network [6].

2.2. STP Topology

The spanning-tree topology is determined by elements such as the unique bridge ID which is made up of the bridge priority and MAC address; the spanning-tree path cost to the spanning-tree root bridge and the port identifier which is also made up of port priority and MAC address. By default, each bridge in the network functions as the STP root when the bridges are powered up. Then, to compute the spanning-tree topology, the bridges send configuration BPDUs through the Ethernet and the radio ports. The BPDUs contain information that helps in computing the spanning-tree topology [6], [12]. The superiority of configuration BPDU is determined by lower values of parameters such as the bridge ID and path cost [6]. Therefore, when a bridge receives a configuration BPDU that contains superior information, then the information is stored for that port and also forwarded with an update message to all attached LANs for which it is the designated bridge if the BPDU is received on the root port of the bridge. However, when the received configuration BPDU contains inferior information compare to the existing one stored for that port, the bridge discards it. Furthermore, if the bridge is a designated bridge for the LAN from which the inferior BPDU was received, then the bridge will send a BPDU containing the up-to-date information stored for that port to that LAN in order to propagate superior information on the network [6].

2.3. Bridge ID, Bridge Priority and System ID Extension

The bridge identity in a network is called the bridge ID. The bridge ID is an 8 byte field which consist of a 2-byte bridge priority field and a 6-byte MAC address field [17]. Each bridge in a network has unique MAC address, however, the bridge priority is configurable. These components of the bridge ID enable each switch to have a unique bridge ID in a network. The analysis is illustrated in the upper part of Figure 1.

The illustration is for a condition in which a spanning tree instance runs for the entire network and it is called Common Spanning-Tree (CST). However, for a large network that implements VLAN, it is essential to run multiple instances of STP in order to accommodate each logical and physical network. The multiple instances of the STP are called Multiple Spanning Tree (MST), Per-VLAN Spanning Tree (PVST) and Per-VLAN Spanning Tree Plus (PVST+). Therefore, when the network is segmented with VLAN, there is need to include information about the VLAN in the bridge ID. This is accomplished by the Extended System ID field which is 12 bits of the original bridge priority that accounts for the respective VLAN participating in the STP [17]. Therefore, summation of the new bridge priority value and the System ID extension is the original bridge priority that is vital in the Root Bridge election process. The analysis is depicted in the lower part of Figure 1 in which the original format has been redefined.

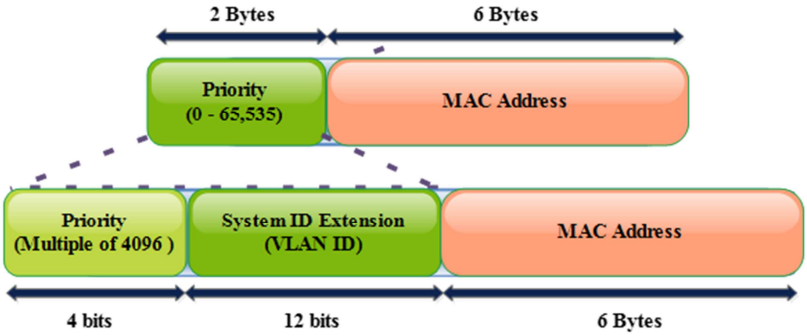


Figure 1. IEEE 802.1D Bridge ID Formats [Adapted from [17]].

3. Root Bridge Election Process

The spanning-tree root is the logical center of the topology. All undesirable paths to the spanning-tree root from any part of the network are placed in the blocking mode. By default, each bridge in the network functions as the STP root when the bridges are powered up. Therefore, each of them claims to be the root bridge in their advertisement. The bridges participating in STP gather information about other bridges in the network through the exchange of BPDU data messages. This messages exchange leads to actions such as the election

of a unique spanning-tree root for each spanning-tree instance, the election of a designated bridge for every Local Area Network (LAN) segment and the removal of loops in the network by blocking redundant Layer 2 interfaces.

Bridges that are initially claiming to be the root bridge will eventually change their status on receiving a Hello BPDU with a lower BID. This Hello BPDU then becomes a superior BPDU. Consequently, the bridge with the lowest numerical priority value and lowest BID is elected as the spanning-tree root for each VLAN in a segmented network [12]. However, in a situation where there is a tie between two switches having the same priority value, then the bridge with the lowest MAC address in the VLAN will eventually become the spanning-tree root bridge [6].

Furthermore, the bridge can be managed by configuring the required lower bridge ID on it in order to make it the root. The bridge priority value is positioned at the most significant bits of the bridge ID. Hence, the probability of the bridge being elected as the root bridge can be manipulated by changing the bridge priority value for it to have a better chance and higher probability of being the root if a lower priority value is configure on it [6].

3.1. STP Port Roles

In a switched network, after the election of the root bridge, each port of the switches in the network is assigned a role depending on its location within the STP topology. According to the 802.1D, roles such as Root Port, Designated Port and Blocked Port can be played by the ports. However, the 802.1w splits the Blocked Port role into Alternate and Backup port roles. After the selection of the best path and the allocation of port roles, all ports with the alternate or backup STP roles will be blocked to prevent loops [10], [13], [18]. Figure 2 depicts the port roles and Table 2 describes different available port roles.

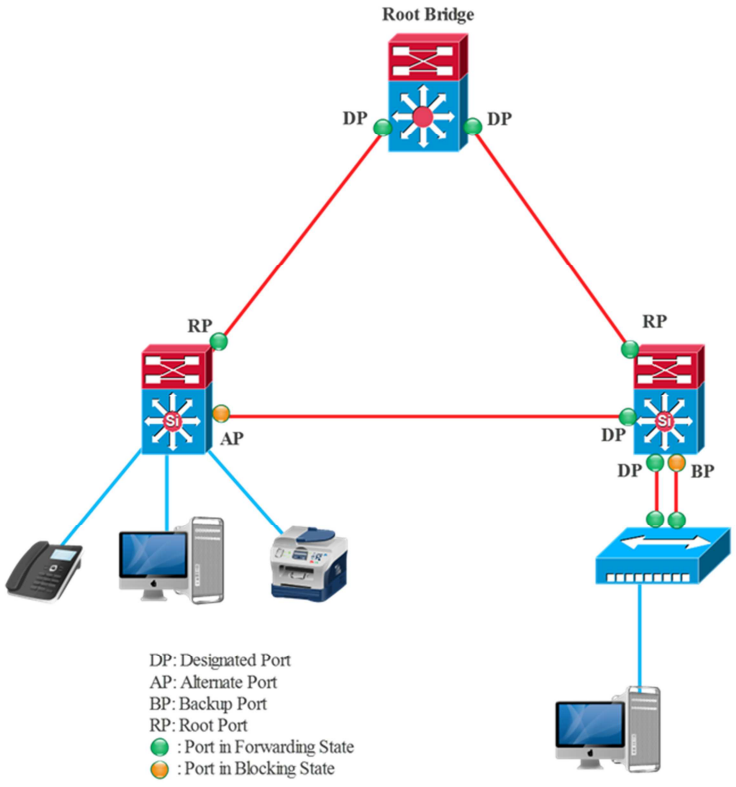


Figure 2. RSTP Bridge Port Roles.

Table 2. RSTP Port Roles.

Port	Description
Root	The root port is the one that receives the best BPDU on each bridge and it is the selected best path to reach the root bridge by non–root ones in the network. Moreover, it should be noted that the root bridge is the only bridge that does not have a root port.
Designated	According to the 802.1D, designated port is chosen because it can send the best BPDU on a specific switched segment. Therefore, it is considered as the best path to the segment. Also, there can only be one designated port per network segment and all the ports on the root bridge are designated.
Alternate	According to its name, it is the alternate path to the root bridge. The alternative port transits to the forwarding state when there is a failure on the root port in order to become the new root port. Furthermore, it receives more useful BPDUs from another bridge than the one that it is on.
Backup	The backup port provides another path to the designated port and take over the designated port role if the current designated port fails. Additionally, it receives more useful BPDUs from the same bridge it is on.

3.2. STP Port States

The ports that are enabled on the network switches participate in spanning-tree topology and they go through a process of interface states before being allowed to forward traffic [10]. This is due to the fact that interface transition directly from nonparticipation in the spanning-tree topology to the forwarding state creates temporary data loops. Consequently, switch interfaces have to wait for new topology information propagation through the LAN before starting to forward frames. In essence, they have to let the frame lifetime expires for forwarded frames that have used the old topology [6]. When the 802.1D STP standard is enabled on the bridge, the Ethernet as well as the radio interfaces pass through the blocking state and the transitory states of listening and learning. The STP then stabilizes each interface at the forwarding or blocking state [6]. However, there are only three port states in Rapid Spanning Tree Protocol (RSTP) - IEEE 802.1w that correspond to the three possible operational states. The 802.1D disabled, blocking, and listening states are merged into a unique 802.1w discarding state. The sequence of 802.1D interface states is shown in Figure 3 while Table 3 compares the 802.1D and 802.1w port states. It should be noted that STP removes redundant links by disabling the ports to which the redundant links are connected and to bring the links up in case of failure leads to convergence issues. Also, the associated bandwidths of the blocked ports are not being utilized in the network. Therefore, to enhance system performance, physical redundant links can be logically grouped into one, thereby, exploiting the available bandwidth with the aid of EtherChannel [5].

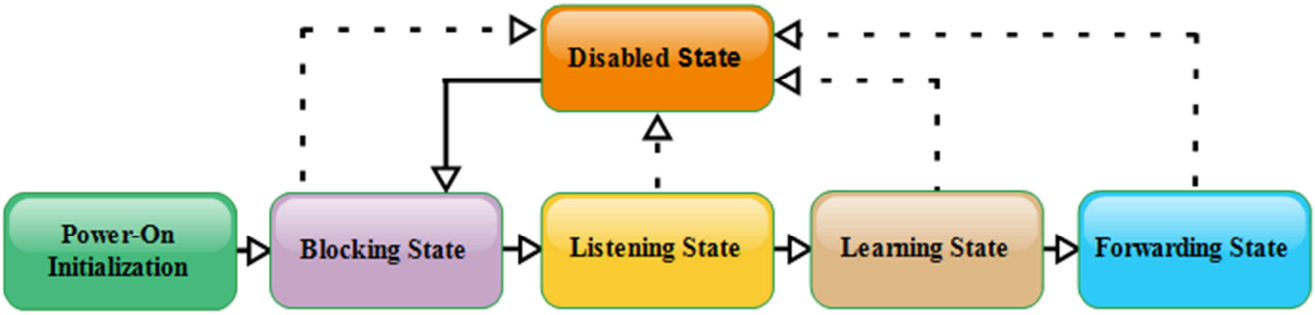


Figure 3. Spanning Tree States (802.1D) [adapted from 6].

Table 3. Comparison of Port States in the 802.1D and 802.1w (Adapted from [18], [19]).

STP (802.1D) Port State	RSTP (802.1w) Port State	Is the Port Included in Active Topology?	Is the Port Learning MAC Addresses?
Blocking	Discarding	No	
Listening	Discarding		
Learning	Learning	Yes	
Forwarding	Forwarding		
Disabled	Discarding	No	

4. EtherChannel

EtherChannel is a technology that offers fault-tolerant as well as high-speed links between network components such as switches, routers, and servers and can be employed to increase the bandwidth between the wiring closets and the data center. Furthermore, it provides automatic recovery for a failed link in the redundant network by redistributing the load across the remaining links. Consequently, when link failure occurs, EtherChannel transmits the traffic automatically from the failed link to the other links in the channel [20]. In essence, to realize a fault-tolerant network, multiple physical Ethernet links such as Fast Ethernet or Gigabit Ethernet links of the switch can be bundled into a single logical link to form an EtherChannel [20], [21].

Each EtherChannel consist of minimum of 2 to maximum of 8 compatibly configured Ethernet interfaces with the same characteristics such as VLAN definition, speed and duplex settings and STP configurations. Therefore, typically, the EtherChannel supports full-duplex bandwidth up to 800 Mbps for the Fast EtherChannel or 8 Gbps for the Gigabit EtherChannel between a switch and another switch or host [20]. It should be noted that STP does not block redundant links when EtherChannel is employed, because, it sees the logical link as a single link. Consequently, EtherChannel implementation helps in bandwidth aggregation by creating a single virtual link that supports the bandwidth sum of each physical link [5]. Hence, it boosts the performance between the two connected network devices. Figure 4 (a) illustrates system without EtherChannel while (b) depicts system that implements EtherChannel. Furthermore, EtherChannel is able to achieve its objective by employing aggregation protocols.

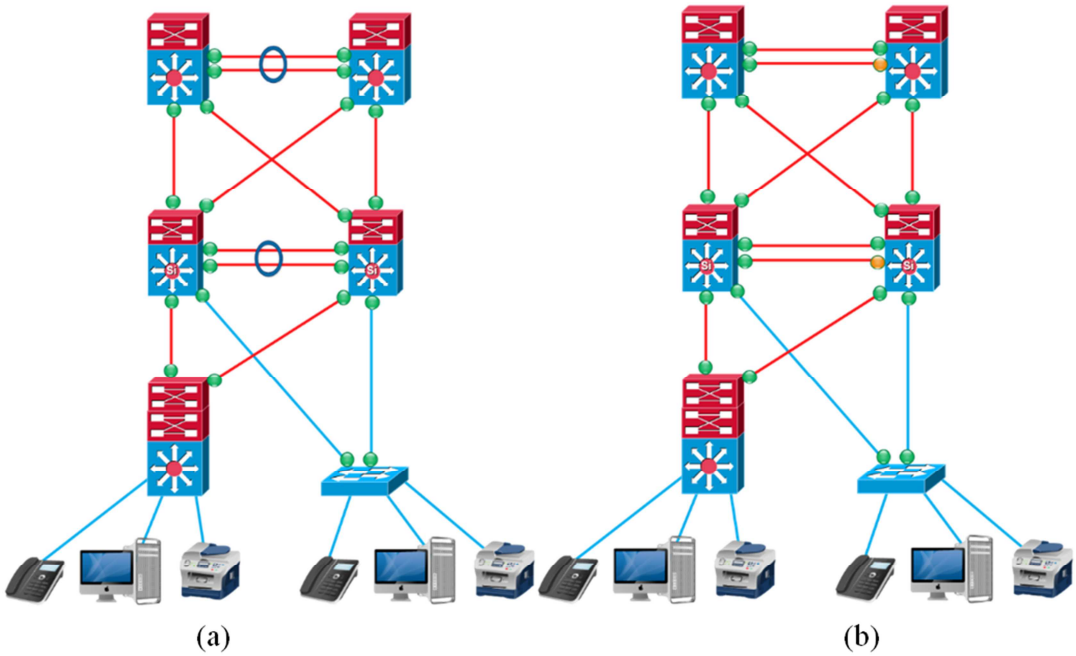


Figure 4. (a) System with Bandwidth Aggregation, (b) System without Bandwidth Aggregation.

4.1. Port Aggregation Protocol and Link Aggregation Protocol

The Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) enable automatic creation of EtherChannels through dynamic exchange of packets between the switch Ethernet interfaces. PAgP is a Cisco-proprietary protocol while LACP is defined in IEEE 802.3AD which is the industry standard implementation [5]. Besides, PAgP and LACP are not compatible, so, both ends of a channel must use the same protocol for a functional EtherChannel establishment. Furthermore, another way of configuring the Etherchannel is through the manual channel configuration without using any form of negotiation.

With the aid of PAgP and LACP, the switch is able to learn about the identity of partners that are capable of supporting either of the protocol as well as the capabilities of their interfaces. Subsequently, similarly configured interfaces are dynamically groups into a single logical link based on factors such as the hardware, administrative, and port parameter constraints [20]. Moreover, for channel establishment, switch interfaces have to be in compatible modes.

4.2. PAgP and LACP Modes

The switch interfaces exchange either the PAgP packets with partner interfaces configured in the auto or desirable modes only or LACP packets with partner interfaces configured in the active or passive modes only. This enables the interfaces to determine EtherChannel establishment based on criteria such as interface speed, trunking state and VLAN numbers for Layer 2 (L2) EtherChannels. Therefore, an EtherChannel can be established between interfaces in as much as they are in compatible modes. However, interfaces that are configured in the ON mode do not exchange PAgP or LACP packets [20]. Table 4 shows the EtherChannel Modes and their descriptions while Table 5 illustrates conditions for channel establishment.

Table 4. EtherChannel Modes (Adapted from [20]).

Mode	Protocol	Description
Active	LACP	It places an interface in an active negotiating state by sending LACP packets to other LACP devices and channel is formed if the other side is in Passive or Active mode.
Passive	LACP	This mode does not start LACP packet negotiation. Thus, it sets the interface into a passive negotiating state but responds to LACP packets received. Channel forms only if the other end is set to Active mode.
Auto	PAgP	Auto mode is a default mode and does not start PAgP packet negotiation. Thus, it sets the interface into a passive negotiating state but responds to PAgP packets received. A channel is formed only if the interface on the other end is set to Desirable mode.
Desirable	PAgP	It places an interface in an active negotiating state by sending PAgP packets to other PAgP devices and channel is formed if the other side is in Auto or Desirable mode.
On	-	Forces the interface into an EtherChannel without any aggregation protocol for negotiation. A functional EtherChannel occurs only when an interface group in the on mode is connected to another group in the on mode.

Table 5. Conditions for Channel Establishment.

Will an EtherChannel be established?		Switch 1				
		Desirable	**Auto**	**Active**	**Passive**	**ON**
Switch 2	Desirable	Yes	Yes	No	No	No
	Auto	Yes	No	No	No	No
	Active	No	No	Yes	Yes	No
	Passive	No	No	Yes	No	No
	ON	No	No	No	No	Yes

5. Experimental Implementation Results and Analysis

This section comprises three sub-section in which the first sub-section presents practical application of PVST to show different STP port roles. Furthermore, the second sub-section illustrates how the root bridge can be managed in a network while the last sub-section shows the implementation of an EtherChannel for bandwidth aggregation. The network is made up of four multilayer switches, two L2-switches, a hub and four PC. For simplicity, only the analyses for part of these devices are presented. The employed network topology shown in Figure 5 is simulated using Cisco Packet Tracer, a graphical network simulator.

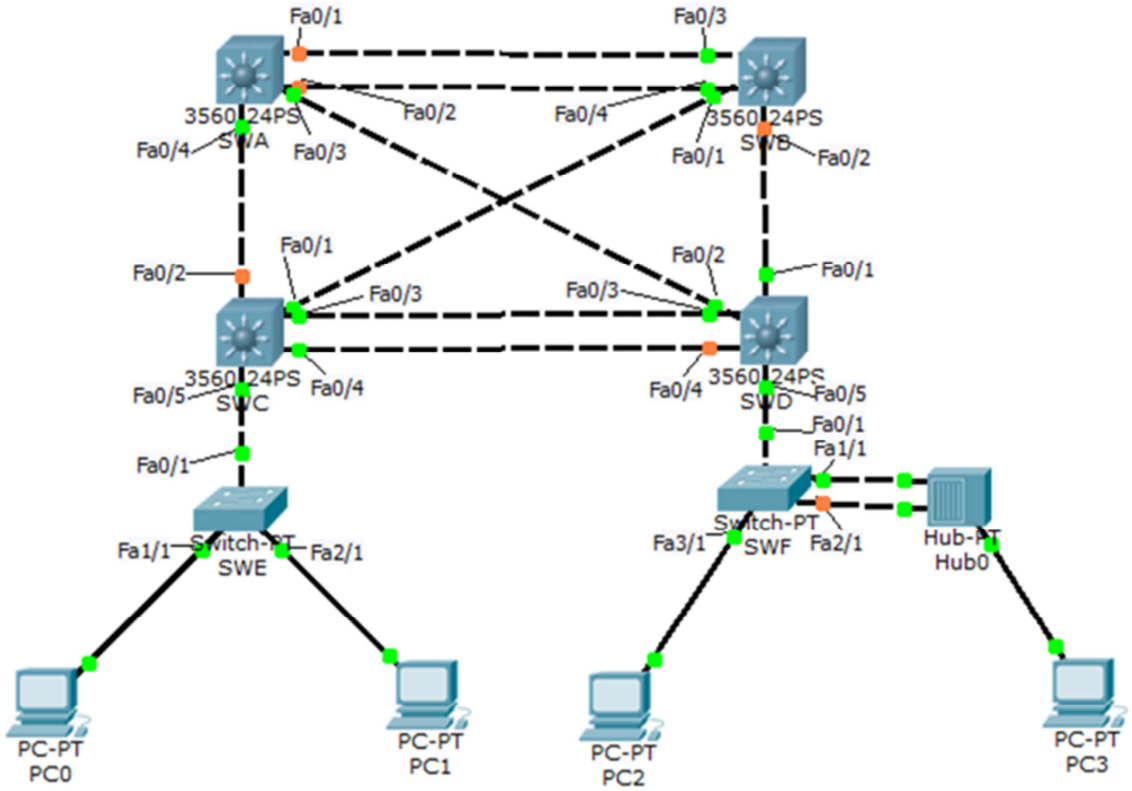


Figure 5. Experimental Network Architecture.

5.1. Experiment 1: Implementation of PVST

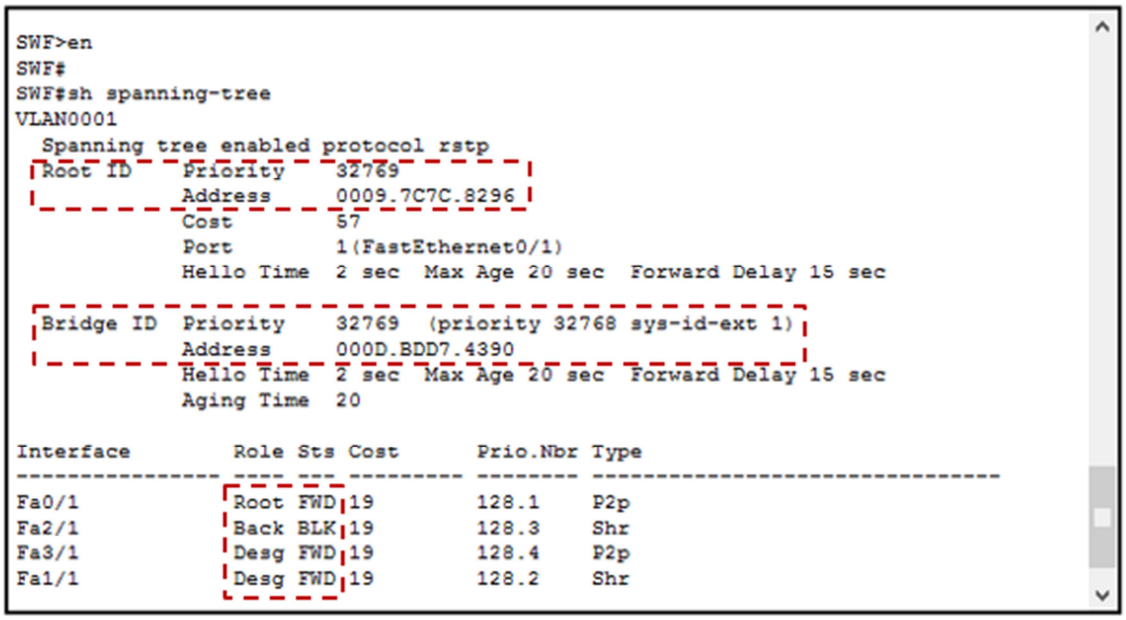
This sub-section demonstrates how to realize different STP port roles with RPVST protocol. Figure 6 highlighted parts show how RPVST can be enabled on a switch and how to confirm that it is running. Also, the highlighted parts of Figures 6 – 8 show different available STP port roles and states. Each of the switch depicts the Bridge ID which represent the actual switch ID and the Root ID which signify the root bridge ID. According to Figures 6 – 8, Switch E is the root bridge. This is also highlighted in Figure 7.

```
SWD#en
SWD#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD(config)#spanning-tree mode rapid-pvst
SWD(config)#^Z
SWD#
%SYS-5-CONFIG_I: Configured from console by console
show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     0009.7C7C.8296
              Cost        38
              Port        3(FastEthernet0/3)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0010.1105.3793
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Root FWD 19        128.3    P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/4            Altn BLK 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
```

Figure 6. Switch D RPVST Configuration with Port Role and State.

```
SWE#
SWE#
SWE#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     0009.7C7C.8296
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0009.7C7C.8296
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa2/1            Desg FWD 19        128.3    P2p
Fa1/1            Desg FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p

SWE#
SWE#
```

Figure 7. Switch E RPVST Configuration with Port Role and State.

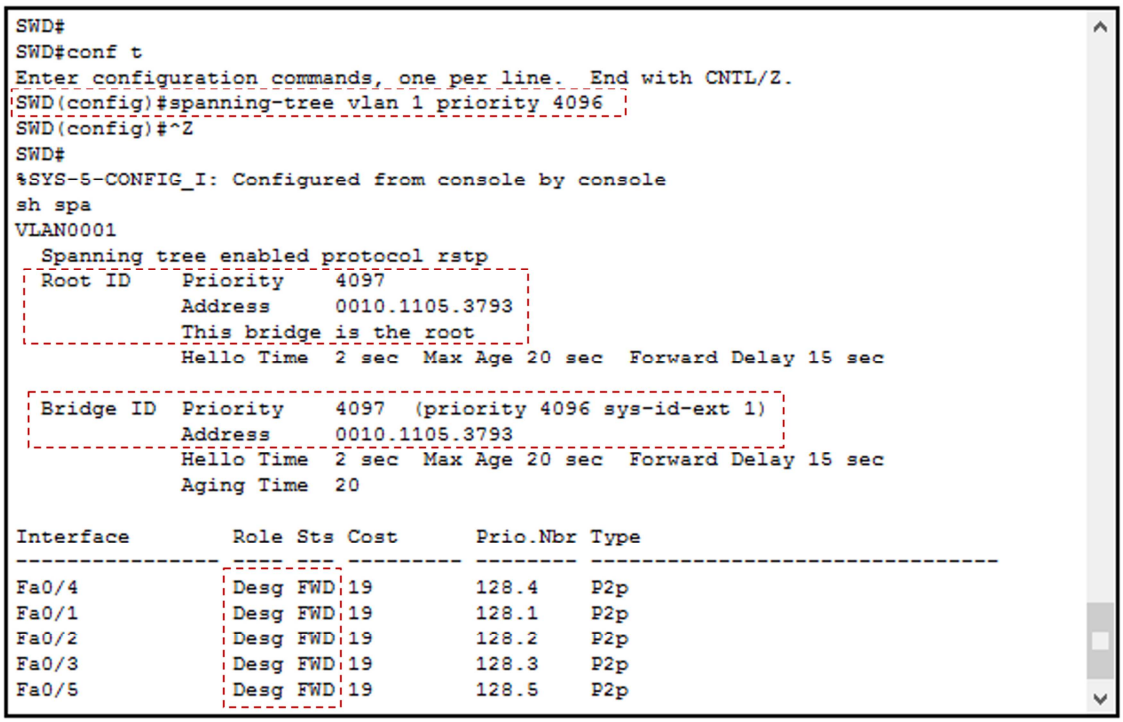


```
SWF>en
SWF#
SWF#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     0009.7C7C.8296
              Cost        57
              Port        1(FastEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000D.BDD7.4390
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa2/1            Back BLK 19        128.3    Shr
Fa3/1            Desg FWD 19        128.4    P2p
Fa1/1            Desg FWD 19        128.2    Shr
```

Figure 8. Switch F RPVST Configuration with Port Role and State.

5.2. Experiment 2: Root Bridge Management

The implementation of RPVST on the topology presented in Figure 5 in the previous experiment makes L2 Switch E the STP root because the priority of all the bridges is set to the default value and Switch E has the lowest MAC address. In a real-life scenario, because of traffic patterns and the link types, this might not be practicable as there are other high-capacity multilayer switches in the network that can offer better performance. Therefore, this sub-section demonstrates a means of controlling the STP root bridge election. To achieve this, Switch D is selected as the ideal bridge for the topology by setting its Bridge Priority to 4096. The highligted part of Figure 9 indicates how to set the Bridge Priority on the switch. Moreover, it shows that Switch D is the new STP root bridge and all of its ports are now playing designated roles and are in forwarding states. Additionally, the highligted parts of Figure 10 shows that the old root bridge, Switch E, has accepted Switch D as the new STP root bridge.



```
SWD#
SWD#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD(config)#spanning-tree vlan 1 priority 4096
SWD(config)#^Z
SWD#
%SYS-5-CONFIG_I: Configured from console by console
sh spa
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    4097
              Address     0010.1105.3793
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4097  (priority 4096 sys-id-ext 1)
              Address     0010.1105.3793
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/5            Desg FWD 19        128.5    P2p
```

Figure 9. Switch D Bridge Priority Configuration with Port Role and State.

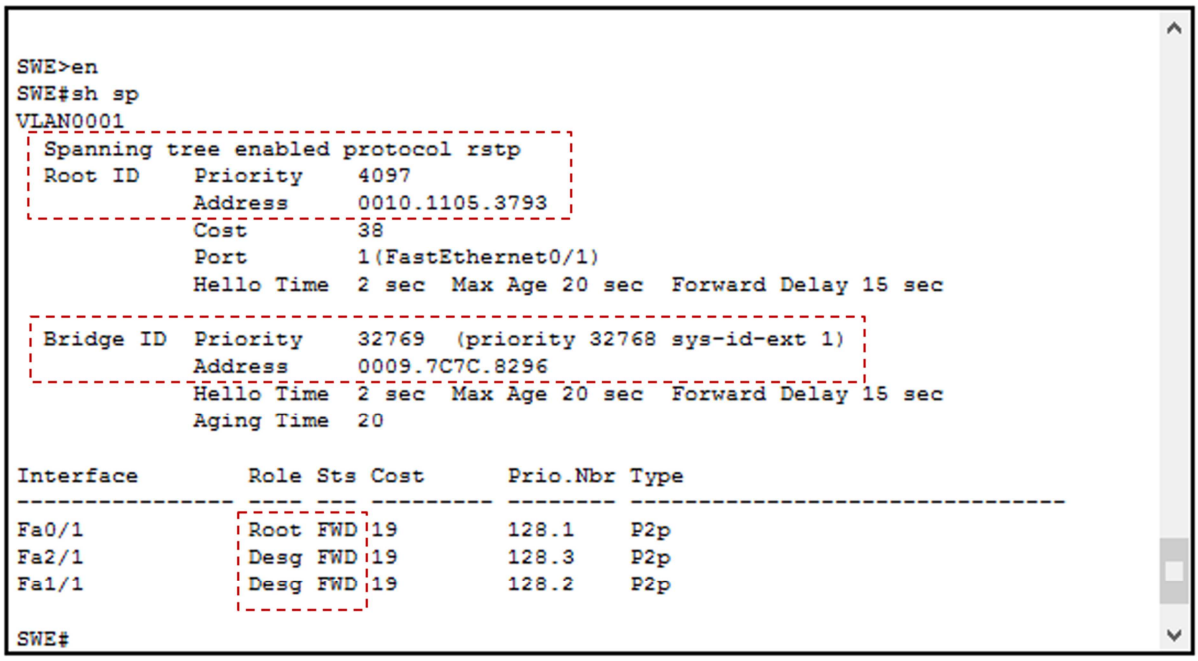


Figure 10. Switch E Port Role and State.

5.3. Experiment 3: Implementation of EtherChannel

This sub-section illustrates the implementation of an EtherChannel for bandwidth aggregation. The redundant links that connect to the root bridge are combined using the EtherChannel configuration as highlighted in Figure 11. Moreover, Figure 12 presents information about the channel-group which includes the protocol employed, the number of ports and maximum number of ports. In the setup, LACP configures the maximum number of LACP-compatible ports in a channel which is up to a maximum of 16 ports. However, only eight LACP links can be active simultaneously. All other additional links are in hot standby in case of failure of the active links. Figure 13 shows that redundant links that connect to the root bridge are in forwarding state and STP does not block them, because, it sees the logical link as a single link. Consequently, EtherChannel implementation helps in bandwidth aggregation.

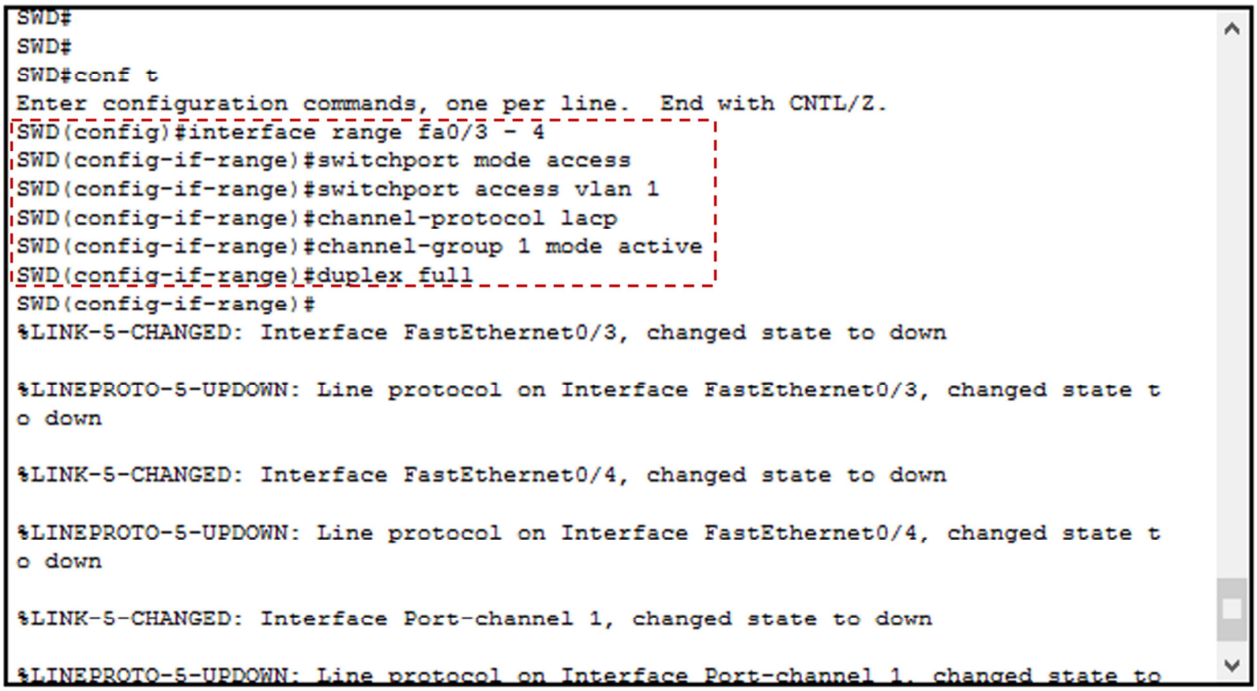


Figure 11. Switch D EtherChannel Configuration.

```
SWD#
%SYS-5-CONFIG_I: Configured from console by console

SWD#sh etherchannel
                Channel-group listing:
                ----------------------

Group: 1
----------
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
SWD#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)           LACP    Fa0/3(P) Fa0/4(P)
SWD#
```

Figure 12. Confirmation of EtherChannel on Switch D.

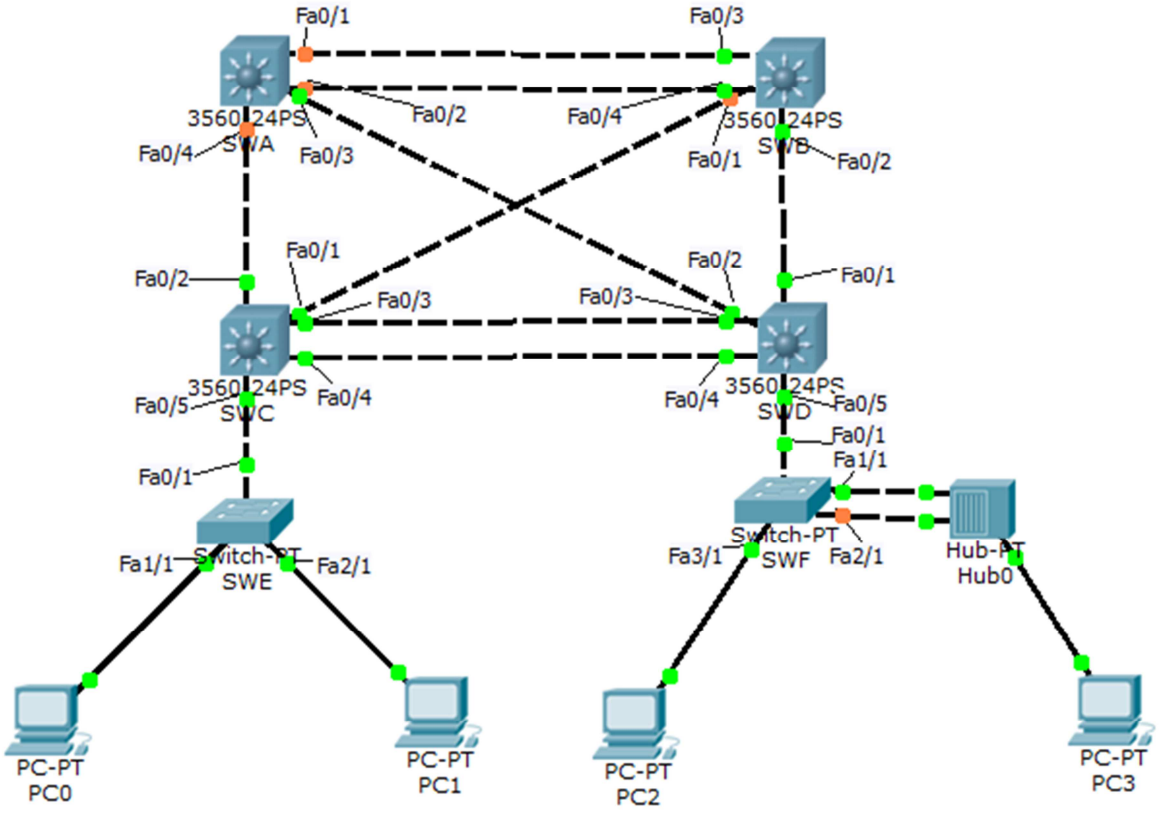


Figure 13. Network Architecture after the EtherChannel Configuration.

6. Conclusions

This paper investigates loop prevention algorithms and bandwidth management in redundant networks by the implementation of spanning tree and EtherChannel protocols. The STP concepts and its implementations in switched networks are discussed. Furthermore, how the root bridge election process can be managed in a network to suit the real-life scenario traffic patterns and the link types is demonstrated. Also, application of an EtherChannel for bandwidth aggregation in order to be able to support various bandwidth intensive multimedia applications and services is presented.

References

[1] I. A. Alimi, A. O. Mufutau and T. D. Ebinowen, "Cost-Effective and Resilient Large-Sized Campus Network Design," *American Journal of Information Science and Computer Engineering,* vol. 1, no. 1, pp.21-32, 2015.

[2] J.M Pedersen, T.P. Knudsen and O.B. Madsen, "Reliability Demands in FTTH Access Networks," *2005 International Conference on Advanced Communication Technology,* vol. 2, pp.1202-1207.

[3] C. Juan, Y. Shuai and M. Hong, "Study and Implementation of Spacewire Network Redundancy Technology based on FPGA," *2014 International Space Wire Conference*, pp.1-5.

[4] Y. Zhuo, P. Yunfeng, L. Keping and L. Yinkai, "On Allocating Redundancy Links to Improve Robustness of Complex Communication Network," *2009 Asia Communications and Photonics Conference and Exhibition,* pp.1-7.

[5] Y.N. Krishnan, C.N. Bhagwat and A.P. Utpat, "Optimizing Spanning Tree Protocol using Port Channel," *2014 International Conference on Electronics and Communication Systems,* pp.1-5.

[6] Cisco Systems, *Cisco 3200 Series Wireless MIC Software Configuration Guide*, Cisco System, 2009.

[7] L.S. Carmichael, N. Ghani, P.K. Rajan, K. O' Donoghue and R. Hott, "Characterization and Comparison of Modern Layer-2 Ethernet Survivability Protocols," *2005 Proceedings of the Southeastern Symposium on System Theory,* pp.124-129.

[8] Cisco Systems, *LAN Switching Configuration Guide (Cisco ASR 920 Series),* 2nd Edition, Cisco System, 2015.

[9] A. Bruno, J. Kim, *CCDA Exam Certification Guide,* 1st Edition, Cisco Press, 2000.

[10] D. Hucaby, D. Donohue and S. Wilkins, *CCNP Switch 642-813 Cert Kit,* 1st Ed., Cisco Press, 2010.

[11] E. Bonada, D. Sala, "RSTP-SP: Shortest Path Extensions to RSTP," *2012 IEEE International Conference on High Performance Switching and Routing,* pp.223-228.

[12] A. Kern, I. Moldovan and T. Cinkler, "Bandwidth Guarantees for Resilient Ethernet Networks through RSTP Port Cost Optimization," *2007 International Conf. on Access Networks & Workshops,* pp.1-8.

[13] R.C. Sofia, "A Survey of Advanced Ethernet Forwarding Approaches," *IEEE Communications Surveys & Tutorials,* vol.11, no.1, pp.92-115, 2009.

[14] A. Gopalan, and S. Ramasubramanian, "Fast Recovery from Link Failures in Ethernet Networks," *IEEE Transactions on Reliability,* vol.63, no.2, pp.412-426, 2014.

[15] R. Pallos, J. Farkas, I. Moldovan and C. Lukovszki, "Performance of Rapid Spanning Tree Protocol in Access and Metro Networks," *2007 International Conf. on Access Networks & Workshops,* pp.1-8.

[16] A. Johnson, *31 Days before Your CCNA Routing and Switching Exam: A Day-By-Day Review Guide for the ICND2 (200-101) Certification Exam,* 3rd Edition, Cisco Press, 2014.

[17] W. Odom, R. Healy, D. Donohue, *CCIE Routing and Switching Certification Guide,* 4th Edition, Cisco Press, 2013.

[18] M.T. Lee, "Feasibility and Performance Analyses of Adapting Ethernet-Based Protocols in Space-Based Networks," *2011 Military Communications Conference,* pp.1845-1852.

[19] Cisco Systems, *Cisco IOS Software Configuration Guide: Cisco IOS Release 15. 1SY,* Cisco System, 2014.

[20] Cisco Systems, *Catalyst 3550 Multilayer Switch Software Configuration Guide: Cisco IOS Release 12.1(13) EA1,* Cisco System, 2003.

[21] R. Froom, B. Sivasubramanian and E.Frahim, *Implementing Cisco IP Switched Networks (SWITCH): Foundation Learning Guide,* 5th Edition, Cisco Press, USA, 2012.

Biography

Isiaka Ajewale Alimi

Isiaka Ajewale Alimi earns B.Tech. (Hons) and M.Eng. in Electrical and Electronics Engineering (Communication) from Ladoke Akintola University of Technology, Ogbomoso, Nigeria in 2001, and the Federal University of Technology, Akure, Nigeria in 2010 respectively. He is a Lecturer in the Department of Electrical and Electronics Engineering, Federal University of Technology, Akure, Nigeria. He has published 3 refereed international journals. He has extensive experience in radio transmission as well as Computer Networking. His research interests include network security, advanced signal processing and wireless communication systems with emphasis on multiple-antenna (MIMO) systems. He is a COREN registered engineer.